

AC

Notice of Allowability

Application No.

09/691,278

Examiner

Paul Callahan

Applicant(s)

PERLMAN ET AL.

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to Interview conducted 12-12-07.
2. ☒ The allowed claim(s) is/are 1-11,13-29,31-47 and 49-54.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

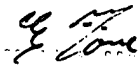
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date 10-17-02 p.c.
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),
Paper No./Mail Date PC
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____


EXAMINER

DETAILED ACTION

1. Claims 1-11, 13-29, 31-47, and 49-57 are pending in the instant Application and have been examined. This Office Action is responsive to the telephonic interview conducted with the Applicant's representatives on December 12, 2007.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Anthony Jones on December 12, 2007.

IN THE SPECIFICATION

On page 7, lines 23-26 are amended as follows:

digital video discs), ~~[[,]] and computer instruction signals embodied in a transmission medium (with or without a carrier wave upon which the signals are modulated).~~
~~For example, the transmission medium may include a communications network, such as the Internet.~~

IN THE CLAIMS

Claims 55, 56, and 57 are cancelled.

Claim 1 is replaced with the following version:

1. A method for operating a key distribution center (KDC) that provides keys to facilitate secure communications between clients and servers across a computer network, wherein the KDC operates without having to store long-term server secrets, comprising: receiving a communication from a server that is authenticated at the KDC; wherein the communication includes a temporary secret key to be used in communications with the server for a limited time period, and wherein the temporary secret key is shared between the server and the KDC; and storing the temporary secret key in a database at the KDC, so that the temporary secret key can be subsequently used to facilitate one or more communications between a client and the server, wherein the temporary secret key is encrypted with a public key belonging to the KDC, so that the temporary secret key can only be decrypted using a private key belonging to the KDC; wherein the temporary secret key is a short-term secret which becomes invalid after a short time period; and wherein the server generates a new temporary secret key in response to a request from the KDC for a new temporary secret key to replace the invalid temporary secret key.

Claim 19 is replaced with the following version:

19. A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for operating a key distribution center (KDC) that provides keys to facilitate secure communications between clients and servers across a computer network, wherein the KDC operates without having to store long-term server secrets, the method comprising: receiving a communication from a server that is authenticated at the KDC; wherein the communication includes a temporary secret key to be used in communications with the server for a limited time period, and wherein the temporary secret key is shared between the server and the KDC; and storing the temporary secret key in a database at the KDC, so that the temporary secret key can be subsequently used to facilitate one or more communications between a client and the server, wherein the temporary secret key is encrypted with a public key belonging to the KDC so that the temporary secret key can only be decrypted using a private key belonging to the KDC; wherein the temporary secret key is a short-term secret which becomes invalid after a short time period; and wherein the server generates a new temporary secret key in response to a request from the KDC for a new temporary secret key to replace the invalid temporary secret key.

Claim 37 is replaced with the following version:

37. An apparatus that provides keys to facilitate secure communications between clients and servers across a computer network, wherein the apparatus operates without having to store long-term server secrets, comprising: a key distribution center (KDC); a receiving mechanism within the KDC that is configured to receive a communication from a server; wherein the communication includes a temporary secret key to be used in communications with the server for a limited time period, and wherein the temporary secret key is shared between the server and the KDC; and a storage mechanism within the KDC that is configured to store the temporary secret key in a database at the KDC, so that the temporary secret key can be subsequently used to facilitate one or more communications between a client and the server, wherein the temporary secret key is encrypted with a public key belonging to the KDC, so that the temporary secret key can only be decrypted using a private key belonging to the KDC; wherein the temporary secret key is a short-term secret which becomes invalid after a short time period; and wherein the server generates a new temporary secret key in response to a request from the KDC for a new temporary secret key to replace the invalid temporary secret key.

Allowable Subject Matter

3. Claims 1-11, 13-29, 31-47, and 49-54 are allowed.

4. The following is an examiner's statement of reasons for allowance:

The closest prior art in the field does not teach the features of the claimed invention of: a server initiating an authentication message exchange with a Key Distribution Center (KDC) where the authentication message contains a temporary secret key to be used in subsequent communications between the server and the KDC, where the temporary secret key is stored in the KDC so as to be used to facilitate communications between a client and the server, where the temporary secret key is stored at the KDC encrypted with a public key of the KDC, where the temporary secret key becomes invalid after a short time period and a new replacement secret key is generated by the server upon request by the KDC. All in the manner of the applicant as found in the independent claims and disclosed in the Applicant's specification.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Paul Callahan

/Paul Callahan/

January 2, 2008

Emmanuel L. Moise
EMMANUEL L. MOISE
SUPERVISOR/ART UNIT EXAMINER